## REMARKS

Applicant wishes to thank the Examiner for reviewing the present application.

Claims 1, 6, 7, 11-13 were rejected under 35 U.S.C. 103(a) as being unpatentable over McCollum (EP0918274A2) in view of Kitaori et al. (US5915024). Applicant respectfully traverses the Examiner's rejection.

As stated in Applicant's previous response, the present invention describes and claims a method of digitally signing a message exchanged between a pair of correspondents where one of the correspondents has a private/public key pair. The method of claim 1 comprises the steps of subdividing the message into a pair of bit strings and utilizing one of the bit strings to compute a first signature component. Using the first signature component and the other bit string, an intermediate signature component is formed. Using the signer's private key and the intermediate component, a second signature component is formed. The first and second signature components, and the other bit string are then combined to provide a signature.

The signature is the output and comprises two computed signature components and a portion of the message (i.e. plaintext) so that the resultant signature has three components. The signature components are used to verify the message, and the plaintext serves as an input for verifying the constructed signature. Not only is the plaintext an integral part of the verification, it also permits information to be conveyed when applied, for example, to a mail item. Therefore, providing a portion of the message in the clear increases bandwidth efficiency when used in certain applications.

As also stated in Applicant's previous response, McCollum teaches a method for securing a data signal having a plurality of signal components. One of the signal components is signed and combined with another signal component. The combined signal is then encrypted and a signature of the encrypted signal is generated to produce an encrypted second signal signature at an output fingerprint. (see col. 4, lines 34-56)

Clearly McCollum does not teach combining two signature components with a plaintext bit string to create an output signature as claimed in claim 1. McCollum teaches generating an entirely different output, namely by encrypting a combined signal and signing the entire encrypted signal to create an output fingerprint. There is absolutely no suggestion in McCollum of sending a portion of a message "in the clear" as plaintext to be used as an input in the verification process. The signature produced by McCollum has a single component, namely the signed encrypted signal, not the three components recited in claim 1. Clearly McCollum cannot anticipate claim 1.

Kitaori teaches using a public/private key pair to create a signature component. However, Kitaori does not teach combining two signature components with a portion of a message "in the clear" to create a signature. Therefore, Kitaori does not teach what is missing from McCollum. The Examiner has suggested that the combination of McCollum and Kitaori teaches claim 1. If one were to take the Examiner's suggestion and combine the teachings of McCollum and Kitaori, the result would still be a signature of an encrypted signal, but at best a combined signal that has been encrypted using the signer's private key (thus an encryption key). It would not be a combination of two computed signature components and a plaintext portion.

There is absolutely no teaching in either reference that would suggest such a step. Applicant respectfully submits that the Examiner has not fully understood what is claimed nor what McCollum and Kitaori teaches. Neither McCollum nor Kitaori alone or in combination teach or even suggest generating a signature from two signature components and a portion of the message.

Therefore, Applicant believes that claim 1 clearly and patentably distinguishes over the combination of McCollum and Kitaori. Claims 2-6 are also believed to distinguish through their dependencies on claim 1.

Claim 7 recites a method for verifying a message subdivided into a pair of bit strings from a signature including at least one component wherein only one of the bit strings is encrypted and the other is not. The other bit string is thus "in the clear" and is used to recover the one of the bit strings.

Again, neither McCollum nor Kitaori teach using a portion of plaintext to verify a message that has been subdivided. There is no suggestion to perform such verification, especially since there is no suggestion of even preparing a signature having a portion which is plaintext.

Accordingly, Applicant believes that claim 7 clearly and patentably distinguishes over the combination of McCollum and Kitaori. Claims 8-13 are also believed to distinguish through their dependencies on claim 7.

Applicant respectfully submits that claims 1-13 are patentable and therefore, are in condition for allowance.

Claim 2 was rejected under 35 U.S.C. 103(a) as being unpatentable over McCollum in view of Kitaori, in further view of Menezes et al. (Handbook of Applied Cryptography), in further view of Nyberg (0639907A1). Applicant respectfully traverses the Examiner's rejection.

Neither Menezes nor Nyberg teach generating a signature by combining two computed signature components with a portion of the message in the clear. Therefore, neither reference teaches what is missing from McCollum and Kitaori. Accordingly, Applicant submits that claim 2 clearly and patentably distinguishes over the combination of prior art cited by the Examiner, and as such, is in condition for allowance.

Claims 3-5 were rejected under 35 U.S.C. 103(a) as being unpatentable over McCollum in view of Kitaori, in further view of Menezes et al. (Handbook of Applied Cryptography), in further view of Nyberg (0639907A1), in further view of ISO/IEC FCD 9796. Applicant respectfully traverses the Examiner's rejection.

Again, the ISO/IEC document fails to teach what is missing from the other applied prior art references. Therefore claims 3-5 are believed to clearly and patentably distinguish over the combination of prior art cited by the Examiner, and as such, are in condition for allowance.

Claims 8-10 were rejected under 35 U.S.C. 103(a) as being unpatentable over McCollum in view of Kitaori, in further view of Nyberg (0639907A1). Applicant respectfully traverses the Examiner's rejection.

As outlined above, Nyberg does not teach what is missing from McCollum and Kitaori, and therefore, claims 8-10 are believed to clearly and patentably distinguish over the combination of prior art. Claims 8-10 are believed to also be in condition for allowance.

In view of the foregoing, Applicant believes that claims 1-13 clearly and patentably distinguish over the various combinations of prior art cited by the Examiner, and as such are in condition for allowance.

In the event that the Applicant's representative has misunderstood the nature of the Examiner's objection or the application of the art, the Examiner is invited to contact the undersigned, to facilitate clarification and avoidance of a final action.

Applicant requests early reconsideration and allowance of the present application.

Respectfully submitted,

Ralph A. Dowell
Agent for Applicant
Registration No. 26,868

Date: July 13, 2005

DOWELL & DOWELL, P.C.
Suite 406
2111 Eisenhower Avenue
Alexandria, VA 22314 USA

Tel: 703.415.2555
Fax: 703.415.2559

21428268.1